COSIC

KU LEUVEN

Post-Quantum Cryptography (PQC): The Risk of Being Late

Bart Preneel
COSIC KU Leuven
Bart.Preneel(at)esat.kuleuven.be @bpreneel1

1 June 2026

SecAppDev

PQCSA

 1

1

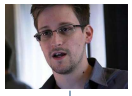
Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- Migration: policy and governance

2

2

Cryptography Timeline



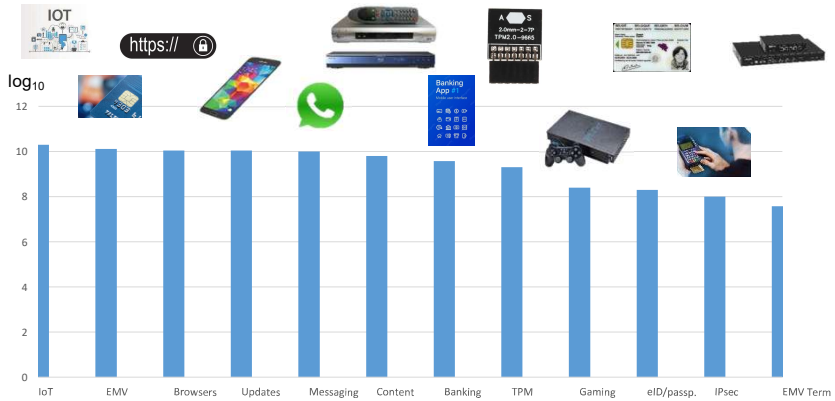
kings, generals & diplomats	wireless & commerce	finance	finance comms	Internet, GSM EMV	crypto-currencies messaging	PQC
pre-1920	1920-1960	1960-1975	1975-1990	1990-2013	2013-2025	2025
mechanical	electro-mechanical	electronics		large-scale adoption	mass adoption end-2-end	ubiquitous

software

3

3

Public-key cryptography deployments ~ 70 B



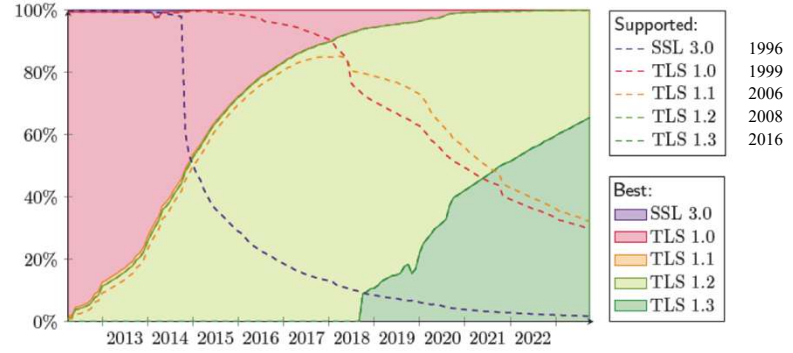
4

4

5

5

TLS migration on top 150K websites



Source: https://www.ssllabs.com/ssl-pulse/

6

6

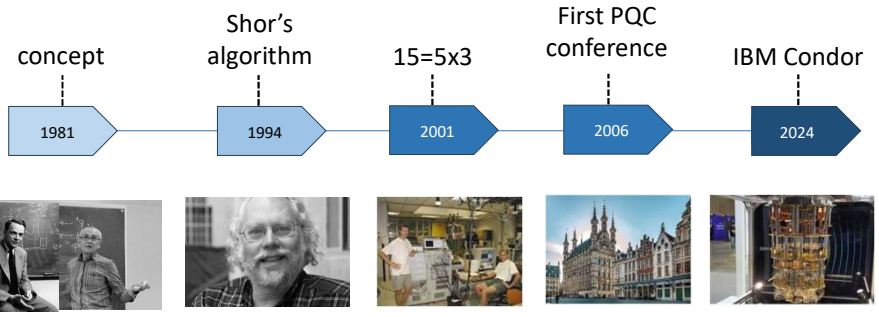
Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- Migration: policy and governance

7

7

Timeline



8

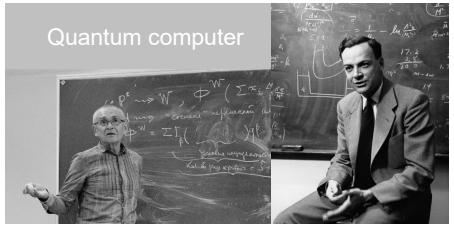
8

The advent of quantum computers

Yuri Manin 1980

Richard Feynman 1981

Exponential parallelism based on entanglement and superposition



Jan. 2014: NSA has spent $85M on research to build a quantum computer

[McKinsey'24] China has spent $14B on quantum technologies (or is it $4B?) versus $3.7B by the US

9

9

If a large quantum computer can be built

public-key cryptography algorithms have to be replaced [Shor'94]

RSA, Diffie-Hellman (including elliptic curves)

Breaking RSA-2048 requires 4096 ideal qubits

≈ 1 million physical qubits (surface codes) https://arxiv.org/abs/2505.15917

≈ 100K physical qubits (QLDPC codes) https://arxiv.org/abs/2602.11457

symmetric crypto: key sizes: x2 [Grover'96]

but huge devices needed; serial algorithm

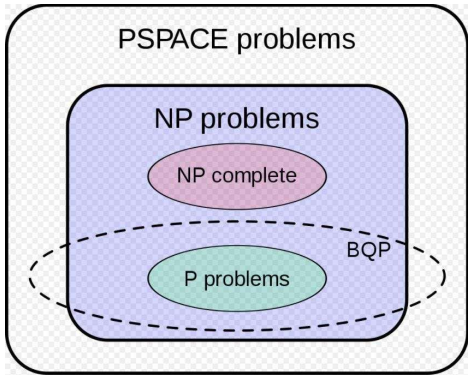
Sam Jacques (CHES'24): don't worry

https://www.youtube.com/watch?v=eB4po9Br1YY

10

10

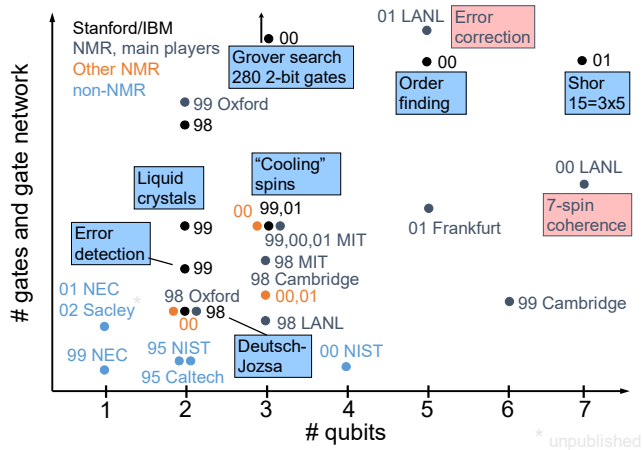
Power of quantum computers: BQP
(Bounded-Error Quantum Polynomial Time)



11

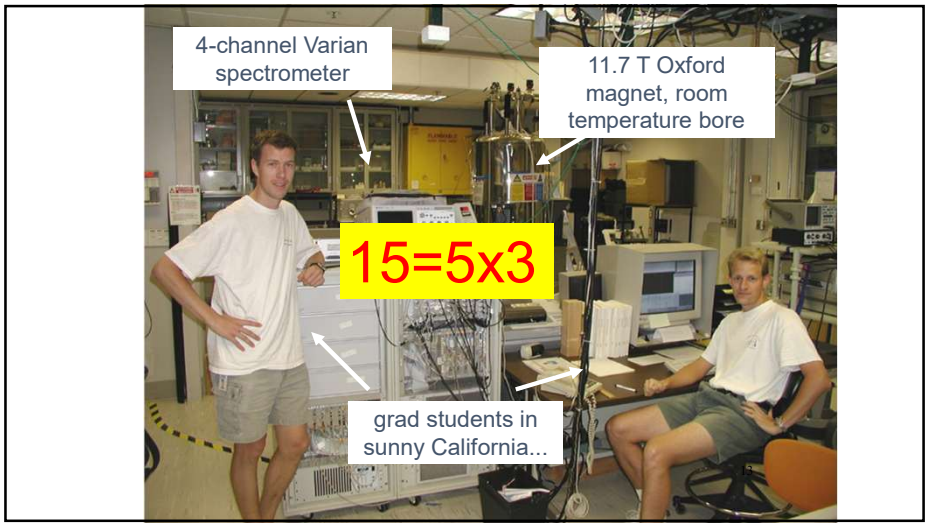
11

State of the art in coherent qubit control ('01)



12

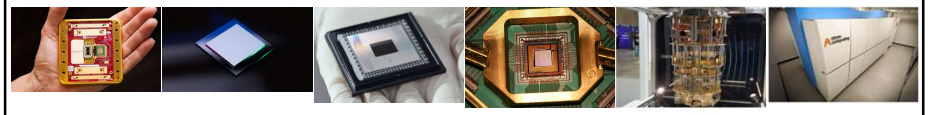
12



13

Quantum computers get names

Microsoft	Amazon	Google	Chinese Academy of Sciences and QuantumCTek	IBM	Atom
Majorana 1	Ocelot	Willow	Tianyan	Condor	
8 qubits	9 qubits	105 qubits	504 qubits	1121 qubits	1180 qubits

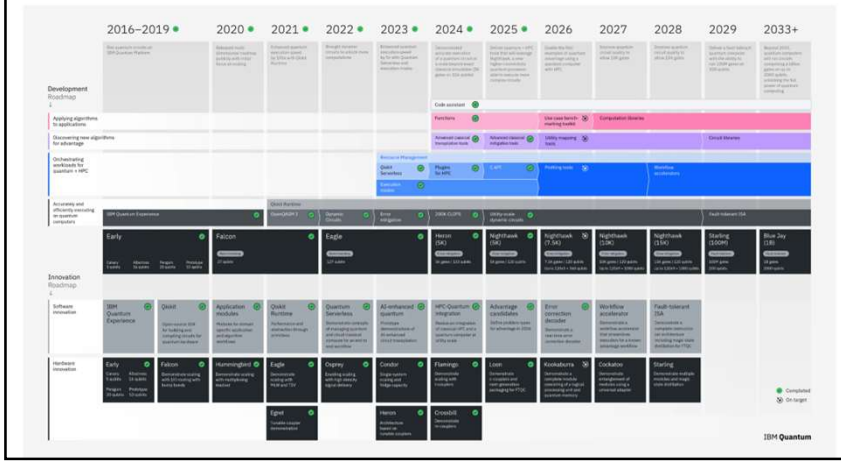


Kookabura
4158 qubits
(announced)

14

14

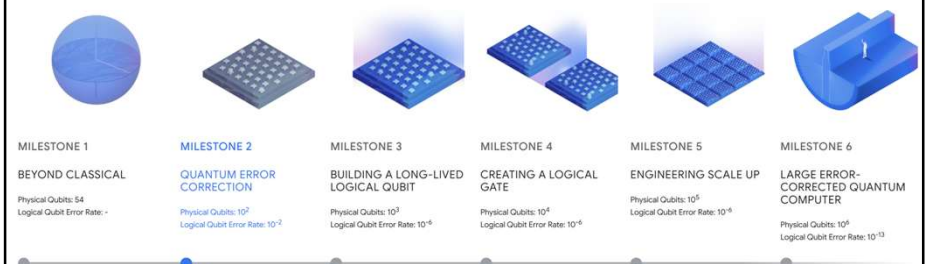
IBM Roadmap (Nov. '25)



15

15

Google Roadmap ('25)



Source: https://quantumai.google/roadmap

16

16

Google

Our Quantum Echoes algorithm is a big step toward real-world applications for quantum computing

Oct 22, 2025 · 5 min read

Our Willow quantum chip demonstrates the first-ever algorithm to achieve verifiable quantum advantage on hardware.

Hartmut Neven, Founder and Lead, Google Quantum AI
Vadim Smelyanskiy, Director, Quantum Pathfinding, Google Quantum AI

Share

17

17

For the first time 1 error-corrected qubit in 2023

Yet researchers have announced in the past two decades lots of simple factorizations on quantum computers: 15, 21, 35, RSA-2048

Paper 2025/1237

Replication of Quantum Factorisation Records with an 8-bit Home Computer, an Abacus, and a Dog

Peter Gutmann, University of Auckland
Stephan Neuhaus, Zurich University of Applied Sciences

Prior work: John A. Smolin, Graeme Smith, Alex Vargo,

- Pretending to factor large numbers on a quantum computer https://arxiv.org/abs/1301.7007
- Published on 10 July 2013 in Nature with as title "Oversimplifying quantum factoring" https://www.nature.com/articles/nature12290

18

18

What does BSI say?

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_2.html?nn=916616

Federal Office for Information Security

Deutschland Digital•Sicher•BSI•

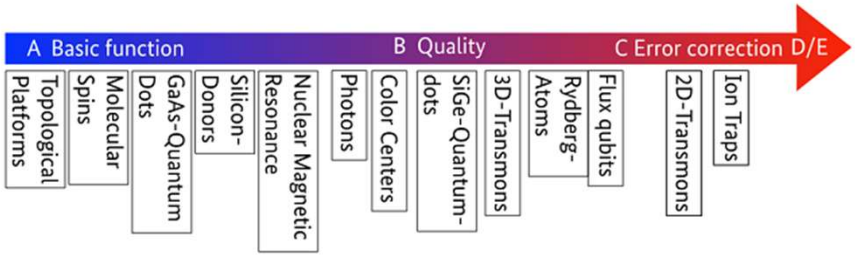
... > Quantum Technologies and Quantum-Safe Cryptography > Status of quantum computer development > The status of quantum computer development

The status of quantum computer development

19

19

BSI Assessment of technologies

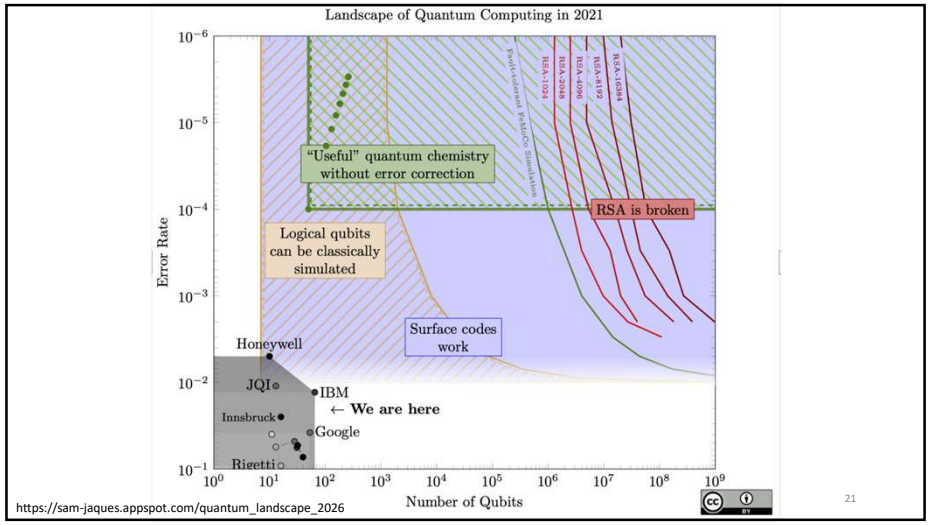


BSI (2025): we estimate at the conservative end that it will take 15 years to build a Cryptographically Relevant Quantum Computer (CRQC)

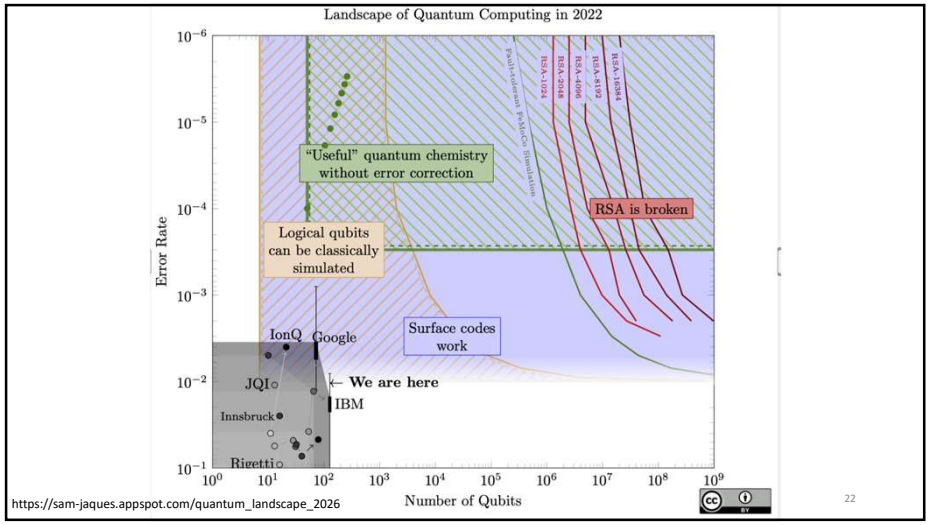
Source: Federal Office for Information Security

20

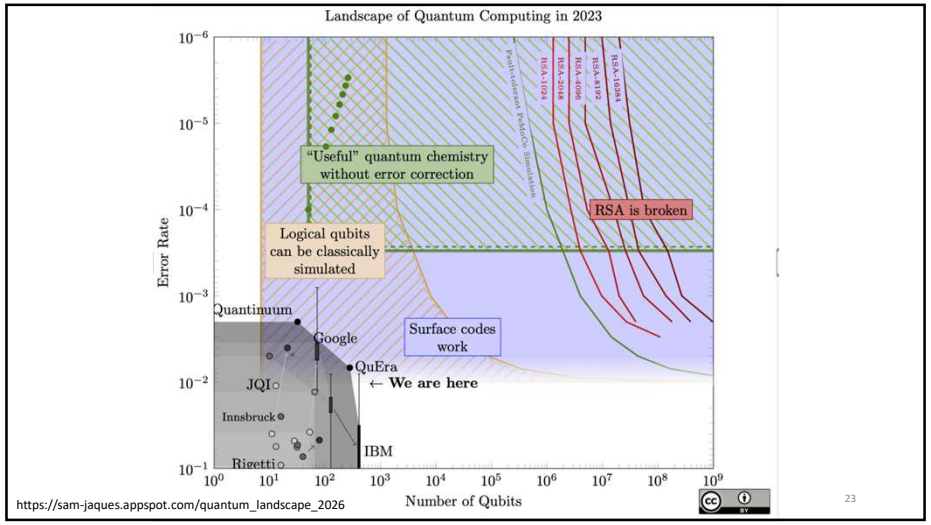
20


Landscape of Quantum Computing in 2021
Error Rate
Number of Qubits
"Useful" quantum chemistry without error correction
RSA is broken
Logical qubits can be classically simulated
Surface codes work
Honeywell
JQI
IBM
← We are here
Innsbruck
Google
Rigetti
https://sam-jaques.appspot.com/quantum_landscape_2026
21

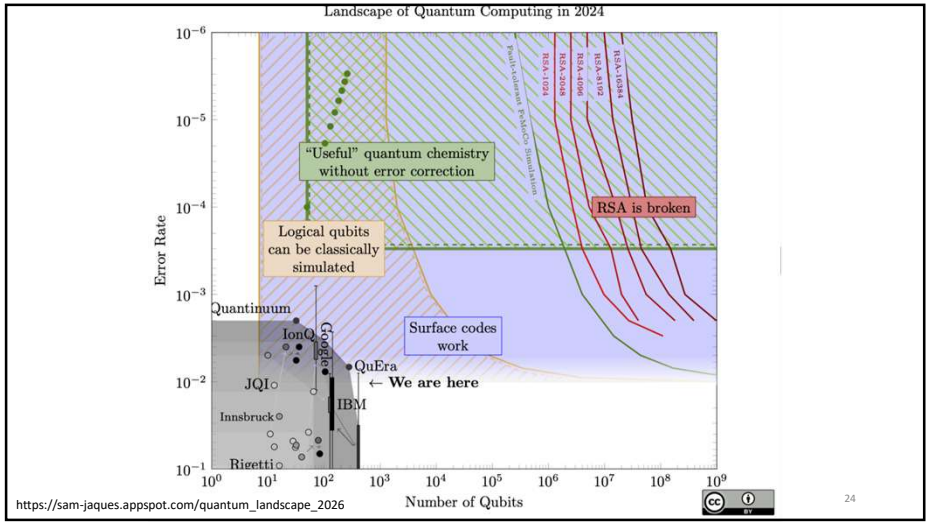
21


Landscape of Quantum Computing in 2022
Error Rate
Number of Qubits
"Useful" quantum chemistry without error correction
RSA is broken
Logical qubits can be classically simulated
Surface codes work
IonQ
Google
JQI
← We are here
IBM
Innsbruck
Rigetti
https://sam-jaques.appspot.com/quantum_landscape_2026
22

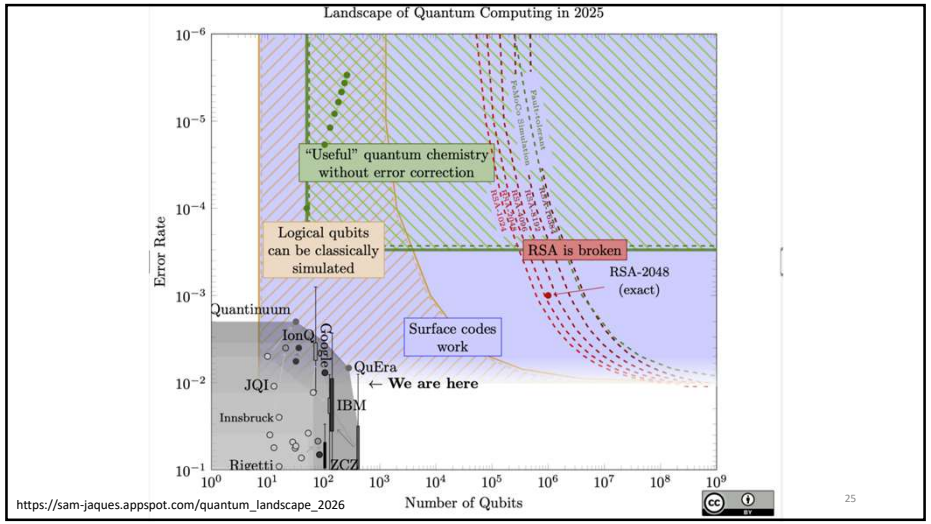
22


Landscape of Quantum Computing in 2023
Error Rate
Number of Qubits
"Useful" quantum chemistry without error correction
RSA is broken
Logical qubits can be classically simulated
Surface codes work
Quantinuum
Google
QuEra
← We are here
JQI
Innsbruck
IBM
Rigetti
https://sam-jaques.appspot.com/quantum_landscape_2026
23

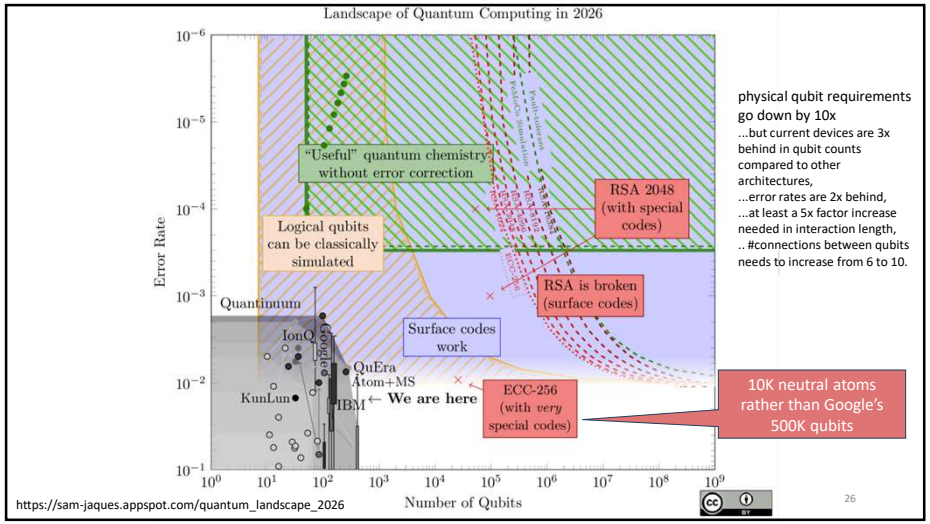
23


Landscape of Quantum Computing in 2024
Error Rate
Number of Qubits
"Useful" quantum chemistry without error correction
RSA is broken
Logical qubits can be classically simulated
Surface codes work
Quantinuum
IonQ
Google
QuEra
← We are here
JQI
IBM
Innsbruck
Rigetti
https://sam-jaques.appspot.com/quantum_landscape_2026
24

24



25

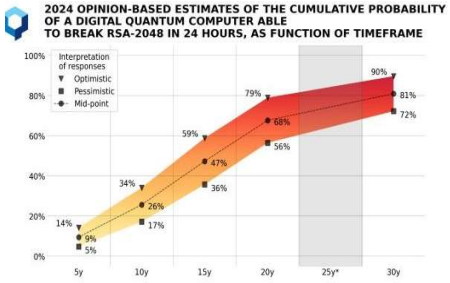


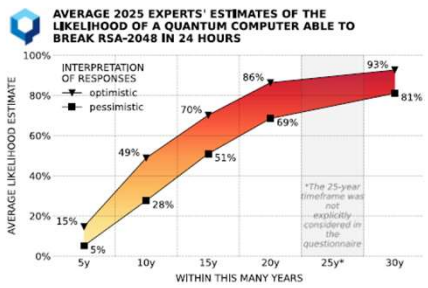
physical qubit requirements go down by 10x
...but current devices are 3x behind in qubit counts compared to other architectures,
...error rates are 2x behind,
...at least a 5x factor increase needed in interaction length,
.. #connections between qubits needs to increase from 6 to 10.

26

What do "the experts" say? (2024-2025)

Source: EvolutionQ





27

27

What do some other experts say?

The Register

You can cross 'Quantum computers to smash crypto' off your list of existential fears for 30 years

RSA's Adi Shamir thinks we're safe for a generation, but more gnarly keys are still a good idea

Iain Thomson Wed 26 Apr 2023 06:28 UTC

RSA CONFERENCE Adi Shamir, the cryptographer whose surname is the "S" in "RSA", thinks folks need to stop worrying about quantum computing breaking encryption algorithms.

Jens Eisert, John Preskill, Mind the gaps: The fraught road to quantum advantage, https://arxiv.org/html/2510.19928v1

28

28

RESEARCH ARTICLE | PHYSICS

Rational quantum mechanics: Testing quantum theory with quantum computers

Tim Palmer | Authors Info & Affiliations

Contributed by Tim Palmer; received August 25, 2025; accepted February 5, 2026; reviewed by Ivette Fuentes, Nicolas Gisin, Lucien Hardy, and Stephen Hsu

March 16, 2026 | 123 (12) e2523350123 | https://doi.org/10.1073/pnas.2523350123

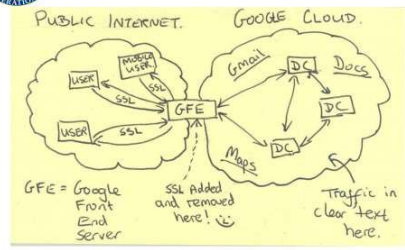
29

29

Muscular (GCHQ) help from Level 3 (LITTLE)

TOP SECRET//SI//NOFORN

Current Efforts - Google

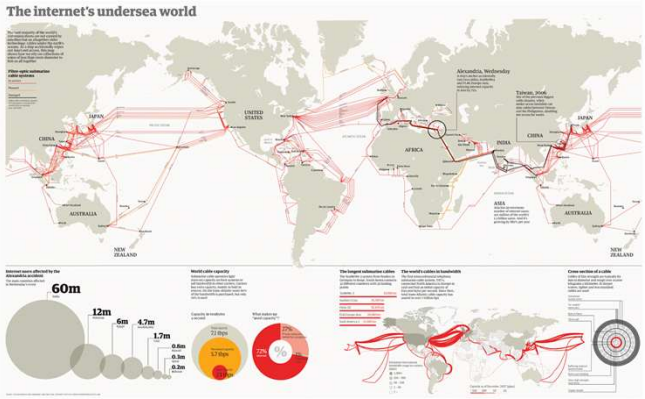


TOP SECRET//SI//NOFORN

Jan 9 2013: In the preceding 30 days, field collectors had processed and sent back 181,280,466 new records — including "metadata," which would indicate who sent or received e-mails and when, as well as content such as text, audio and video (from Yahoo! and Google)

30

Upstream: 90% of traffic over cables



GCHQ plan in 2009:
tap 16.9Tbs
select 3.9Tbs (egress)
~20%

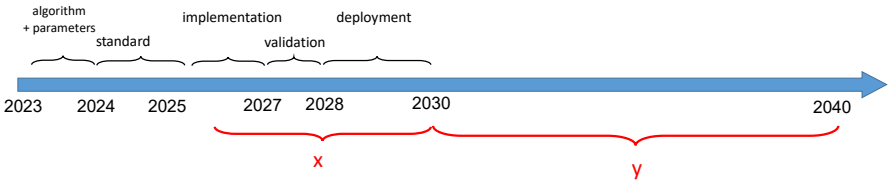
31

When to switch to post-quantum cryptography? [Mosca]

Q = #years until first large quantum computer
x = #years it takes to switch (3-12 years)
y = #years data needs to be confidential (10 years)

Need to start switching in the year 2026 + Q – x – y
e.g. Q = 14, x=4, y=10: today!

For digital signatures, y ≈ 0



32

Who is your adversary?

- Nation states
- Organized crime
- Competitor

What is their target?

- Top secret info
- Business critical data
- Your shopping list?

Will they tell you when they have a CRQC?

33

33

Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- Migration: policy and governance

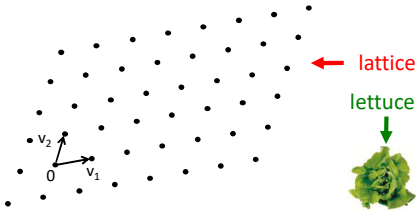
34

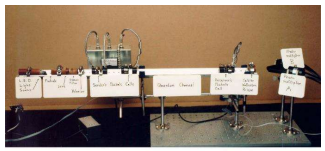
34

Post-quantum Cryptography ≠ Quantum Key Distribution

Find new cryptographic algorithms that resist attacks on quantum computers

Use quantum physics to agree on secret keys





Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

35

35

NIST Post-Quantum Competition (2016-2026)

https://en.wikipedia.org/wiki/Post-Quantum_Cryptography_Standardization
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Encryption: KYBER
Digital signatures: Dilithium, Falcon, SPHINCS+ (hash-based signature)

	Signatures	Encryption/KEM	TOTAL
Lattice	4/3/2/2	24/9/3/1	28/12/5/3
Code	5/0/0/0	19/7/1/0	24/7/1/0
Multivariate	7/4/1/0	6/0/0/0	13/4/1/0
Hash	4/1/0/1	0/0/0/0	4/1/0/1
Other	3/1/0/0	10/1/0/0	13/2/0/0
TOTAL	23/9/3/3	59/17/4/1	82/26/7/4

IETF (independent of NIST): 2 hash-based signatures
- RFC 8554 Leighton-Micali signatures
- RFC 8391 XMSS eXtended Merkle signatures

36

36

COSIC researchers break high profile candidates

A New Attack Easily Knocked Out a Potential Encryption Algorithm

SIKE was a contender for post-quantum-computing encryption. It took researchers an hour and a single PC to break it.

Wouter Castryck, Thomas Decru
Microsoft bounty of 50.000$

Paper 2022/214

Breaking Rainbow Takes a Weekend on a Laptop

2024/1297 (PDF)

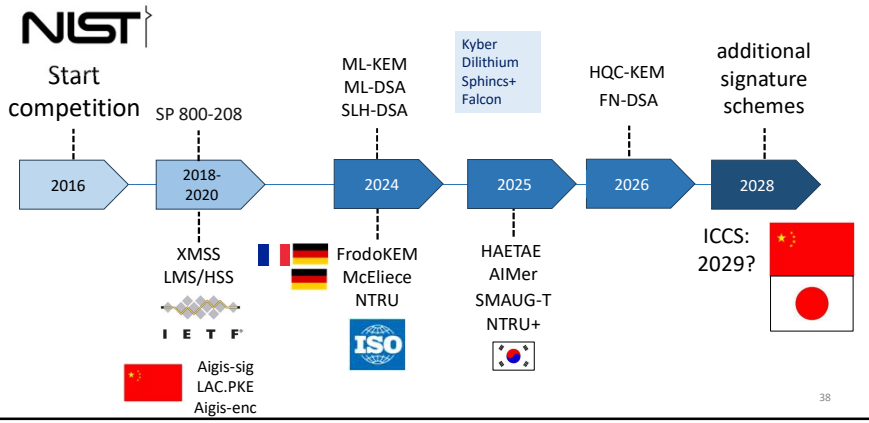
Improved Cryptanalysis of SNOVA

Ward Beullens
(second result at IBM)

37

37

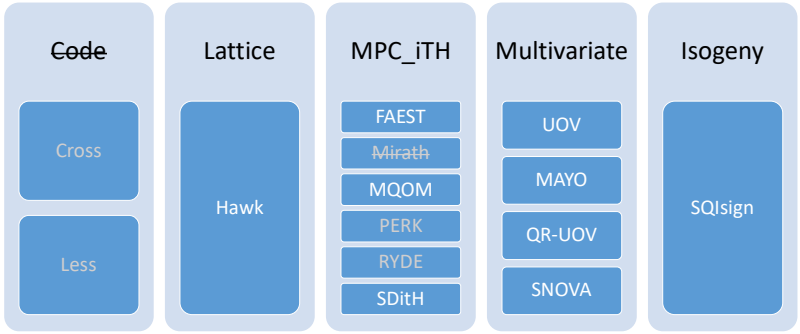
PQC Algorithm Standardization



38

38

NIST: Round 3 of Digital Signatures (part II)



39

39

40

New scheme: larger sizes but not slower

Key agreement/encryption:

- **Key size + ciphertext x3..x15**
- Encryption: 2x slower than RSA, 5x faster than ECC
- Decryption faster

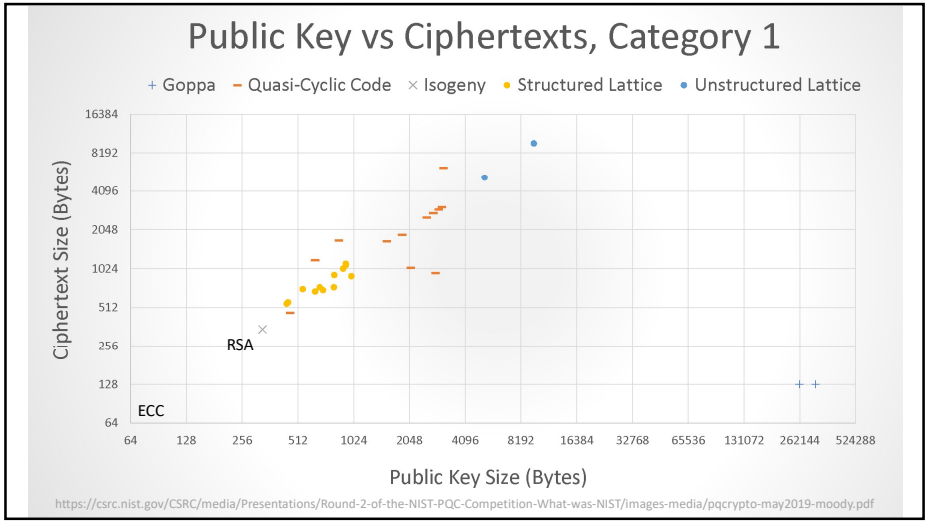
Signatures

- **Public key + signature x15..x30**
- Signing faster
- Verification: comparable to faster

Under development: ZK, OPRF, VPRF, PAKE, threshold signatures,…

40

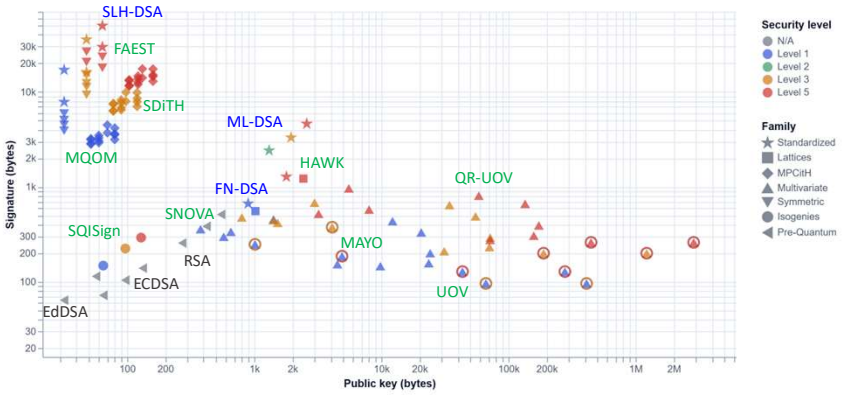
40



41

Digital Signature comparison

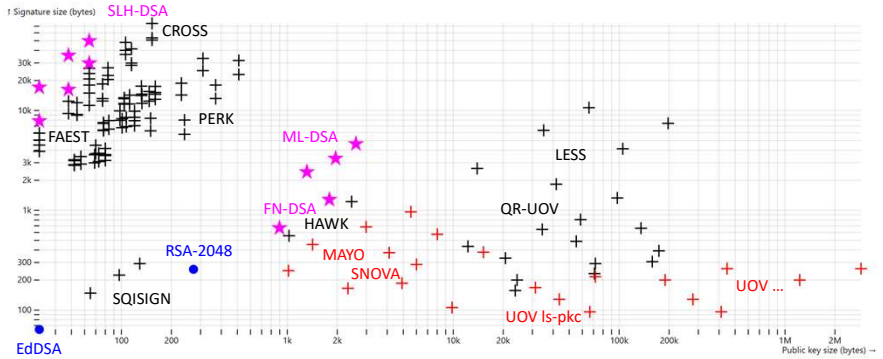
source: Signature Zoo (Tom Wiggers) https://pqshield.github.io/nist-sigs-zoo/



42

Digital Signature comparison

source: Signature Zoo (Tom Wiggers) https://pqshield.github.io/nist-sigs-zoo/



43

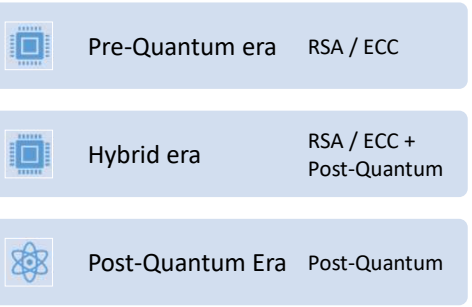
Digital Signature comparison

source: Signature Zoo (Tom Wiggers) https://pqshield.github.io/nist-sigs-zoo/

Scheme	Security	Public key + signature (byte)	Sign + Verify (relative to ML-DSA)
ECC (Ed25519)	X	96	0.14
Factoring (RSA)	X	528	40.2
Lattice (ML-DSA)	OK	2733	1.00
Symmetric (LMS) (3)	OK	1160	5.65
Lattice (FN-DSA 512)	Maybe	1563	1.85
Multivariate (MAYO) (8)	?	1874	1.4
Isogeny (SQISIGN)		241	177.5
Lattice (HAWK)		1579	0.73
Code (CROSS)	?	7994	27.5
MPC (Ryde) (5)	?	7532	27.5
VOLE (FAEST)	?	5728	12

44

How to continue?



	OR: gradual transition	AND: no gradual transition
Digital signature	Ok	Long term secure
Public key encryption	No long term security	Long term secure

Migration 60 billion libraries and applications in billions of devices

45

45

Additional challenges

- Most robust schemes and higher security levels have worse performance: SLH-DSA and Classic McEliece
- Lattice based schemes: ML-KEM, ML-DSA, FN-DSA
  - Decryption failure, floating point, noise sampling
- Side channel resistance:
  - KyberSlash
  - EM in Fujisaki-Okamoto mode: FO-calyps [Azouaoui et al., Surviving the FO-CALYPS: Securing PQC Implementations in Practice, RWC'22]
  - …

46

46

Are we done yet? (1/3)

- IETF: TLS, IPsec (IKEv2), SSH, JOSE, COSE, messaging:
  - there is no direct PQC alternative for Diffie-Hellman (built-in forward secrecy)
  - only KEM, no signatures yet
  - future may be KEM-based protocols
- LINUX foundation: Post-Quantum Cryptography Alliance (PQCA)
  - open quantum safe (OQS) project
  - post-quantum crypto VPN (fork of OpenVPN)
  - post-quantum TLS (fork of OpenSSL)
  - post-quantum SSH (fork of OpenSSH 7.7)
- TCG: Lattice based Direct Anonymous Attestation (draft)

47

47

Are we done yet? (2/3)

- Threshold signatures: NIST
- Blind signatures: IS 18370
- Anonymous signatures: IS 20008
  - Direct anonymous attestation
  - Group signatures
  - Ring signatures
- Oblivious transfer: IS 25330
- ZK Proofs
- Identity and credentials: W3C, DIF, FIDO
- Multi-Party Computation (MPC): IS 4922

48

48

Are we done yet? (3/3)

- Oblivious PRF
- Verifiable PRF
- Password Authenticated Key Establishment (PAKE)

49

49

Outline

- Cryptography
- The Quantum Threat
- Post-Quantum cryptography
- Migration: policy and governance

50

50

PQC = A huge software migration project:
slow, expensive and complex
does not bring in new revenue

- Risk-based analysis (cannot do it all)
- Crypto-inventory is first step but extremely complex – most organizations depend on suppliers who will not move synchronously
- Gradations of complexity – 10-year agenda
  - Relatively easy: messaging, network security (TLS, SSH) underway
  - Difficult: digital signatures for secure boot/update
  - Hard: PKI e.g. middleboxes and clients break when certificate chains larger than 10kB (ML-DSA: 15 kByte)
  - Hard: platforms
- End-game should be crypto-agility

51

51

KEMs are easier than signatures

- **Encryption:** ML-KEM satisfactory (but some avoid ML-KEM-512)
  - AES-128: needs no upgrade but AES-256 combined with PQC requires level 5: 2x storage and 2x slower
- **Digital signatures**: ML-DSA default but more issues (some avoid ML-KEM-44)
  - Prehashing
  - Private key format: seed, key, seed + key

IETF draft has gone from 26 to 18 variants of which 6 are recommended (RFC ready in May 2026)

52

52

Browsers/TLS: hybrid KEM by default

March'24	Chrome on Desktop
Nov'24	Android and Firefox
Apr '25	OpenSSL
Oct '25	Apple iOS, iPadOS, macOS
Oct'25	Signal Sparse Post Quantum Ratchet

Source: https://research.cloudflare.com/about/people/bas-westerbaan/

53

53

Post-quantum encryption in TLS as observed by Cloudflare

Other stats
18 million TLS connections per second
38% of top 100K webservers
Only 3.7% of Cloudflare origins

source: https://radar.cloudflare.com/adoption-and-usage

54

54

Digital signature applications

- Code updates
- TLS 1.3 handshake has 5 signatures and 3 public keys (7-9 Kbyte)
  - Handshake signature
  - PKI 2 signatures for the certificate chain
  - 2 signatures for certificate transparency
- PKI: will need hybrid certificate and classical certificate to allow for smooth upgrade
- HSM: hardware upgrade then certification then deployment

55

55

Merkle Tree Certificates for TLS

https://davidben.github.io/merkle-tree-certs/draft-davidben-tls-merkle-tree-certs.html
https://blog.cloudflare.com/bootstrap-mtc?trk=public_post_comment-text/

- TLS handshake: has 5 signatures and 3 public keys (7-9 Kbyte)
  - Larger PQC certificates/timestamps: 200 bytes -> 7 kbytes
  - Shorter certificate lifetimes (reduce revocation challenges)
  - Large certificate transparency trees (auditable logging of certs)
- Idea: first log a cert (hashes of public keys) and then sign a batch (reverse order)
- Cert: 1 signature + 1 public key + 1 inclusion proof
- Signed treeheads can be predistributed (shared by many certs) – even shorter than today
  - signatureless certificates - inclusion proofs in Merkle trees (relying party needs additional info)

56

56

Microsoft | Microsoft On the Issues Our Company News and Stories 1

Post-quantum resilience: building secure foundations

Aug 20, 2025 | Amy Hogan-Burney - CVP, Customer Security & Trust

Quantum frontiers may be closer than they appear

Mar 25, 2026 2 min read

We're setting a timeline for post-quantum cryptography migration to 2029.

Heather Adkins VP, Security Engineering

Sophie Schmieg Senior Staff Cryptography Engineer

Google

Share

Cloudflare targets 2029 for full post-quantum security

2026-04-07

Bas Westerbaan

57

57

What did the NSA say in Sept.'22?

https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

AES-256, SHA-384, SHA-512
LMS/XMSS
CRYSTALS-Kyber, CRYSTALS-Dilithium level V

National Security Agency | Cybersecurity Advisory

Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary

The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break

CNSA 2.0

Public-key
CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates
Extended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

		2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Software/firmware signing	transition			Support and prefer						Exclusive		
Networking (VPN/routers)												
Web browsers/servers												
Operating systems												
Niche (IoT, PKI)												
Custom applications & legacy	No hybrid mode!									Update/replace		

58

What did the NIST propose in Nov.'24?

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

	Security level	2025-2030	2031 - 2034	2035-
RSA-2048, DH, MQV	112		Deprecated	Disallowed
ECDSA, ECDH, MQC	112			
RSA-3072, DH, MQV	128			
ECDSA, ECDH, EdDSA	128			
PQC or **Hybrid**	128-256			

59

What did the White House say (17 Jan.'25)?

https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-01470.pdf

Presidential Documents

Executive Order 14144 of January 16, 2025

Strengthening and Promoting Innovation in the Nation's Cybersecurity

- Secure BGP, DNS
- Encrypt email
- End to end encryption of voice and video conferencing
- TLS 1.3 requirement
- Agencies shall implement PQC key establishment or hybrid key establishment including a PQC algorithm **as soon as practicable** upon support being provided by network security products and services already deployed in their network architectures

60

What did the White House say (6 Jun.'25)?

https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

December 1, 2025: release of a regularly updated CISA list of product categories that support PQC
January 2, 2030: issue requirements for agencies to support TLS 1.3 or higher (if available)
Removed

- PQC support requirements in product solicitations
- adopting PQC or hybrid KEM as soon as practicable
- language on international collaboration

61

Rumours (20 May'26): New draft Executive Order

https://postquantum.com/post-quantum/pqc-timeline-compression/

December 31, 2030: key agreement
December 31, 2031: digital signatures

62

Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

Canadian National Quantum-Readiness
BEST PRACTICES AND GUIDELINES
Version 04 10 July 2024

63

What did the EU say? (Apr.'24)

https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronised transition among the different Member States and their public sectors.

Call by 18 EU Member States (Nov'24)

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf

Roadmap for Member States by 2026

Projects: PQCSA and PiQASO

64

European Cybersecurity Certification Group: Agreed Cryptographic Mechanisms (v2.0 April 2025)

https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf

- **Good:** Adds lattice-based schemes Frodo-KEM and ML-KEM in hybrid mode
- **Bad:** Phasing out RSA-2048 (up to RSA-2999) for encryption by the end of 2025!
- **Ugly:** transparent process for public review is missing

65

NIS Cooperation Group A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (Part 1, v1.1, 23 June '25)

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

First steps by 31 December 2026: awareness, risk analysis, plan

Distinction: low risk, medium risk, high risk

High risk: 2030	Medium risk: 2035	Low risk: try by 2035

66

EU and cryptography: a difficult marriage

- Export control: what is **weak** cryptography
  - Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
- European Cybersecurity Certification Group (EUCC): Agreed Cryptographic Mechanisms: what is **very strong** for all member states (Common Criteria)
- No algorithm/protocols paper with recommendation for **"normal"** users
  - exist at national level
  - informal documents 2005-2020 (ECRYPT and ENISA)

COSIC 67

67

More EU

- GDPR
- CRA: September 2026
- DORA

68

G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector

13 January 2026 https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

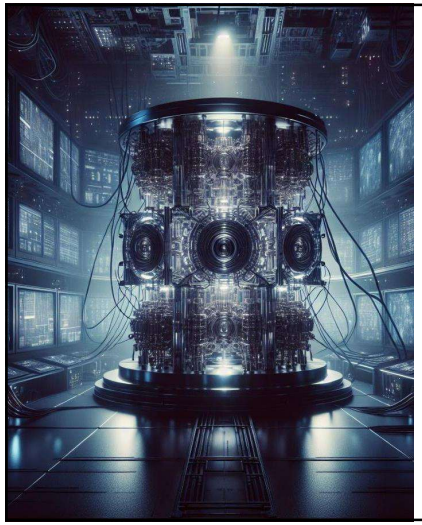
69

By sector

70

- Government: should have started in 1994 for level secret and above
- Health: long term confidentiality
- Finance: driven by regulators (Singapore, Israel, Bank of England, ECB, BAFIN)
- Automotive: long product life cycles – software updates

70



Conclusion

- We do not know for sure if or when a quantum computer will break RSA & ECC
- But there seems to be a consensus that we can't take the risk
- Need to move:
  - risk-based approach
  - crypto-agility
  - EU-level strategy
- Quantum computers will bring many cool applications
- But it still can take a while

71

71

Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN

COSIC

72

Links

NIST/NSA

- https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-postquantum-cryptographic-algorithms
- https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

GSMA

- https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/
- https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
- https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Jan '20

- https://sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf (EU level Common Criteria agreement)

BSI

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html

Canada

- https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

Australia

- https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

73

73

More links

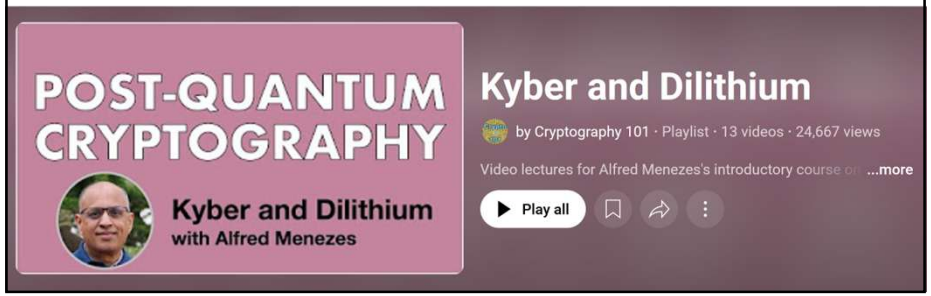
- Quantum Computing Roadmap overview: https://postquantum.com/quantum-computing-roadmaps-2025/#company=aegiq&company_id=24540
- Critical comments:
  - https://arxiv.org/abs/1301.7007
  - https://www.nature.com/articles/nature12290
  - https://eprint.iacr.org/2025/1237
- EU Draft roadmap https://digital-strategy.ec.europa.eu/en/news/survey-eu-roadmap-post-quantum-cryptography
- https://blog.cloudflare.com/another-look-at-pq-signatures/
- https://github.com/IETF-Hackathon/pqc-certificates
- https://datatracker.ietf.org/doc/draft-ietf-pquip-hbs-state/

74

74

Lectures on PQC by Alfred Menezes

https://www.youtube.com/playlist?list=PLA1qgQLL41SSUOHlq8ADraKKzv47v2yrF



75